UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,131	09/04/2001	Boris Balacheff	30001505-4	9453

22879 7590 09/29/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
09/29/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte BORIS BALACHEFF and DAVID CHAN

Appeal 2009-006386
Application 09/936,131
Technology Center 2400

Before JOHN C. MARTIN, MAHSHID D. SAADAT, and
BRADLEY W. BAUMEISTER, *Administrative Patent Judges*.

MARTIN, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

This is an appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-26, 28-38, 42, 43, 45, 46, and 48-61. Final Action 1, Office Action Summary. Claim 27 stands objected to for depending on a rejected claim. *Id.* at 21.

We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

A. Appellants' invention

Appellants' invention relates to a method of operating a computing entity such that a user of the entity is confident that the computing entity is in the trusted state. Specification 1:5-8.

Figure 1 of the Application is reproduced below.

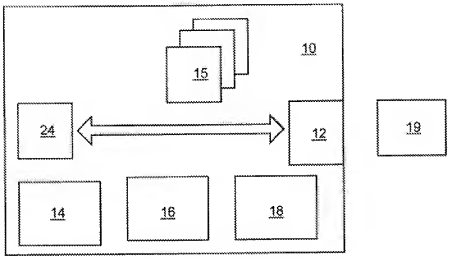


FIGURE 1

Figure 1 is a block diagram showing a "trusted computing platform 10" (*id.* at 13:35; 14:12-13). Computing platform 10 includes, *inter alia*, the

standard features of a keyboard 14, mouse 16, monitor 18, and smart card reader 12 for reading a smart card 19 (*id.* at 13:35–14:5). Smart card 19 is also referred to in the Specification (*e.g.*, *id.* at 22:8) and the claims (*e.g.*, claim 1) as a "token device." Computing platform 10 further includes a trusted device 24 (Specification 15:20), which is incorporated into the computing platform in order to bind the identity of the platform to reliably measured data that provides an integrity metric of the platform (*id.* at 12:24-27).

Figure 2 is reproduced below.

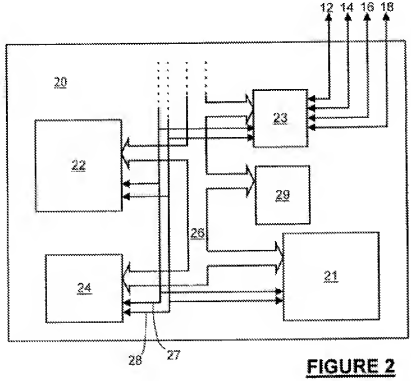


FIGURE 2

Figure 2 is a block diagram of a motherboard 20 of trusted computing platform 10 (*id.* at 14:12-13). The motherboard includes, *inter alia*, the trusted device 24, a main processor 21, a main memory 22, a data bus 26 and

respective control lines 27 and lines 28, a BIOS memory 29 containing the BIOS program for the platform 10, and an Input/Output device 23 (*id.* at 14:12-19).

Figure 3 is reproduced below.

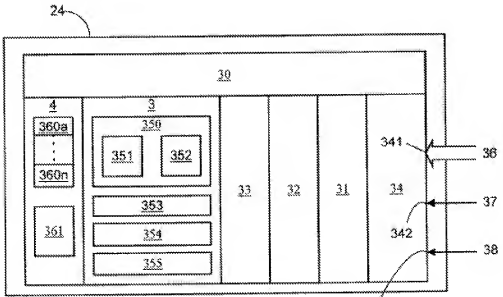


FIGURE 3

Figure 3 depicts the components of trusted device 24 (*id.* at 16:8-9). The trusted device includes, *inter alia*: a controller 30 programmed to control the overall operation of the trusted device 24; a measurement function 31 for acquiring an integrity metric from the platform 10; a cryptographic function 32 for signing, encrypting, or decrypting specified data; an authentication function 33 for authenticating the smart card; and interface circuitry 34 having appropriate ports (36, 37, 38) for connecting the trusted device 24 respectively to the data bus 26, control lines 27, and address lines 28 of the motherboard (*id.* at 16:18-26). Trusted device 24 also

has volatile memory areas 4 and/or non-volatile memory areas 3 (*id.* at 16:26-28).

The trusted device 24 "is equipped with at least one method of reliably measuring or acquiring the integrity metric of the computing platform 10 with which it is associated" (*id.* at 17:13-15). In one embodiment, the integrity metric is acquired by the measurement function 31 by generating a digest of the BIOS instructions in the BIOS memory (*id.* at 17:15-17). Such an acquired integrity metric, if verified, gives a potential user of the platform 10 a high level of confidence that the platform 10 has not been subverted at a hardware, or BIOS program, level (*id.* at 17:17-19).

B. The claims

The independent claims before us are claims 1, 17, 18, 25, 32, 38, 42, 43, 48, and 59. Claim 1 reads as follows:

> 1. A system of computing apparatus comprising:
>
> a computing platform having a first data processor and a first data storage means;
>
> a monitoring component having a second data processor and a second data storage means, *wherein said monitoring component is configured to perform a plurality of data checks on said computing platform*; and
>
> a token device being physically distinct and separable from said computing platform and said monitoring component,
>
> wherein in one mode of operation, said token device operates to make an integrity challenge to said monitoring component and said token device will not undertake specific

> actions of which it is capable unless it receives a satisfactory response to said integrity challenge.

Claims App. A-1 (Br.) (emphasis added).

In describing the support for claim 1 in their Application, Appellants read the recited "computing platform" on platform 10, the "monitoring component" on trusted device 24, and the "token" on smart card 19. (Br. 3.)

C. The references

The Examiner's rejections are based on the following references:

Perlman	US 6,230,266 B1	May 8, 2001
Audebert	US 6,694,436 B1	Feb. 17, 2004

D. The rejections

Claims 1, 2, 10-26, 28-32, 38, 42, 43, 45, 46, and 48-61 stand rejected under 35 U.S.C. § 102(e) for anticipation by Audebert. Final Action 4.[2]

Claims 3-9 and 33-37 stand rejected under 35 U.S.C. § 103(a) for obviousness over Audebert in view of Perlman. (Answer 19.[3])

Appellants' arguments are limited to the anticipation rejection of the independent claims.

---

[2] The statement of the rejection at page 4 of the Final Action incorrectly includes cancelled claims 41, 44, and 47.

[3] The statement of this ground of rejection at page 19 of the Final Action omits claim 35, which depends on claim 34.

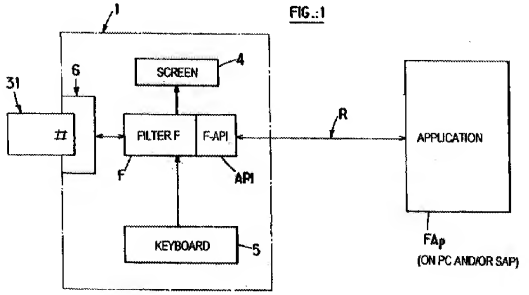
THE ISSUE

The principal issue raised by Appellants' arguments is whether the recited "data checks on said computing platform" (claim 1) must be performed at the location of the computing platform.[4]

ANALYSIS

Audebert discloses a terminal and system for performing secure electronic transactions (title).

Figure 1 of Audebert is reproduced below.



[4] *See Ex parte Frye*, 94 USPQ2d 1072, 1075 (BPAI 2010) (precedential) ("If an appellant fails to present arguments on a particular issue — or, more broadly, on a particular rejection — the Board will not, as a general matter, unilaterally review those uncontested aspects of the rejection."). Designated precedential at
(Continued on next page.)

Figure 1 is a diagram showing the functional architecture of Audebert's system (col. 8, ll. 23-24). The system includes a terminal module 1 and a personal security device 31 (abstract) in the form of an integrated circuit card (col. 9, l. 13) or smart card (col. 19, ll. 4-5). Terminal module 1 can be a dedicated terminal or integrated into a PC or into a network computer (NC) dedicated to network applications or into a cable TV network decoder (Set Top Box) (col. 9, ll. 28-31).

Terminal module 1 is adapted to receive high-level requests from an application Fap (also FAp[5]) installed on an electronic unit (abstract). Application FAp can be installed on the server Sap (on-line mode) or a PC or NC available to the user (off-line mode, for example signing of electronic mail) (col. 9, ll. 59-62). In on-line mode, terminal module 1 is connected to the server Sap, on which the application FAp, is installed via the PC and a network R, such as the Internet (col. 9, ll. 36-41). System security is provided by filter F (discussed below) in terminal module 1 (col. 10, l. 24).

The Examiner, comparing claim 1 to Audebert, reads the recited "computing platform" on server Sap, the "monitoring component" on terminal module 1, and the "token device" on card 31. Final Action 4. Thus, in contrast to the above-described embodiment depicted in Appellants' Figures 1-3, in which trusted device 24 (i.e., the recited "monitoring component") is described as a *part* of trusted computer platform 10,

---

http://www.uspto.gov/ip/boards/bpai/decisions/prec/index.jsp.

[5] Audebert, col. 9, l. 16.

Audebert's server Sap, on which the Examiner reads the recited "computer platform," is located remotely from terminal module 1, i.e., the recited "monitoring component."

The Examiner interprets the claim language as broad enough to read on using the filter F of terminal module 1 to analyze data received by terminal 1 from server Sap in order to identify, verify, or authenticate Application FAp on the server or the "source" or "origin" of the requests sent by Application FAp on the server. Specifically, Audebert, in describing filter F in terminal module 1, explains that:

(a) "[t]he filter program includes a unit for identifying and/or authenticating the source of requests sent by the application (Fap) installed in the electronic unit" (abstract, ll. 16-18);

(b) the device for executing the filter program "comprises first means for identifying and/or authenticating said application installed on said unit or the source of said requests sent by said application" (col. 7, ll. 5-8)[6]; and

(c) a high-level request from server Sap to terminal module 1 can contain a single elementary command to be transferred to the personal security device and also "a Message Authentication Code that will enable the filter F to check the origin and integrity of this request before sending the elementary command to the personal security device" (col. 10, ll. 7-14).

Appellants argue that

[6] This feature is also recited in Audebert claim 2 at column 28, lines 20-25, cited at page 22 of the Answer.

> while the terminal of Audebert does indeed verify the integrity of data received from the server, this is not the same as performing data checks on the server. The terminal of Audebert first receives data from the server and then, once the received data is in its possession, verifies its integrity – in other words, the terminal performs data integrity checks on the terminal, not on the server. This is not a mere matter of semantics; by performing data checks on the computing platform, the claimed invention assures the integrity of the platform itself, whereas the approach of Audebert can do no more than verify the integrity of the received data.

(Br. 8.) We understand Appellants to be arguing that the claim language "perform a plurality of data checks on said computing platform" requires performing the data checks *at the location* of the recited "computer platform" (i.e., server Sap) rather than at the location of the recited "monitoring component" (i.e., terminal module 1), as occurs in Audebert. The Examiner responded by stating (1) that "[the] claims do not recite or specify *how* the data check and the verification operation are being performed" (Answer 22 (emphases altered)), and (2) that "according to claims 19 and 23 [dependent on claim 18], the monitoring component *receives* some information related to the computer platform in order to perform either data check or verification operation on the computer platform, which is the same [as] what [is] being taught in Audebert" (*id.* (emphases altered)).

We agree with Appellants' argument that this interpretation of claims 19 and 23 is incorrect. Neither claim describes "receiving" data at the "monitoring component" from the "computer platform," let alone analyzing the received data in order to perform the recited "data checks" on the

computing platform.[7] Nevertheless, we do not agree with Appellants that claim 1 requires performing the data checks at the location of the computer platform. The claim language "wherein said monitoring component is configured to perform a plurality of data checks *on* said computing platform" (emphasis added) is broad enough to read on performing data checks "about" or "regarding" the computing platform, e.g., by checking data received from the computing platform by the monitoring component. Furthermore, because claim 1 does not specify that a data check is performed to check the "integrity" of the computer platform, we are not persuaded by Appellants' argument that "verifying the *origin* of data is not the same as verifying the *integrity of the origin* of data." (Br. 9.)

For the foregoing reasons, we will sustain the rejection of independent claim 1, the rejection of independent claims 17, 18, 48, and 59, as to which Appellants (Br. 9) repeat their claim 1 arguments, and the rejections of dependent claims 2-16, 19-24, 45, 46, 49-58, 60, and 61, which are not separately argued. *In re Nielson*, 816 F.2d 1567, 1572 (Fed. Cir. 1987).

---

[7] Claims 19 and 23 read as follows (emphases added):

19. The computing entity as claimed in claim 18, wherein on communication between said token device and said interface means, said monitoring component is activated to perform a monitoring operation on said computer platform, in which *said monitoring component obtains data describing an operating status of said computer platform.*

23. The computing entity as claimed in claim 18, wherein said *monitoring component comprises a verification means configured to obtain a certification data* independently certifying said status data, and to provide said certification data to said interface means.

Claim 25, which is separately argued, reads as follows:

> 25. A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform comprising a first data processor and a first memory means, and a monitoring component comprising a second data processor and a second memory means, said method comprising the steps of:
>
> *receiving an interrogation request signal via an interface of said comput*[*er*] *entity*;
>
> said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal; and
>
> said monitoring component reporting a result message to said interface, said result message describing a result of said monitoring operation.

(Emphasis added.)

In describing the support in their Application for this claim, Appellants read the recited "interface" on smart card reader 12, the "computer platform" on platform 10, and the "monitoring component" on trusted device 24. (Br. 4.)

The Examiner reads the recited "interrogation request signal" on the high-level requests sent from Audebert's Application FAp on server Sap to terminal module 1 (the recited "monitoring component") and reads the recited "monitoring operation of said computer platform" on terminal module 1's authentication of the *origin* of the request, i.e., the server. Final Action 3, para. 2. Thus, the Examiner is reading the claim language as broad enough to

permit the monitoring component (Audebert's terminal module 1) to receive an interrogation request signal from the computer platform (Audebert's server Sap) and then to respond to such a request by "performing a monitoring operation of" the computer platform (again, server Sap).

We are not persuaded by Appellants' arguments against the Examiner's position. One argument is that "there is in fact no interrogation request signal received by the server (computing platform) of Audebert; on the contrary, the requests in Audebert flow from the server to the terminal." (Br. 9.) While this is an accurate description of the direction of requests between Audebert's server and monitoring terminal, this argument incorrectly suggests that claim 25 requires the interrogation request signal to be received by the "computer platform," which the Examiner reads on Audebert's server Sap. Instead, claim 25 recites "receiving an interrogation request signal via an interface of said *comput[er] entity*" (emphasis added), which term the claim explains comprises the computer platform *and* the monitoring component.[8] As a result, we agree with the Examiner that the "receiving" step is broad enough to permit the interrogation request signal to be received (via an interface) by the monitoring component (i.e., Audebert terminal module 1) rather than by the computer platform (server Sap).

Appellants ask, "If the terminal unit is the monitoring component (as the Examiner asserts on page 10 of the final Action), then what corresponds

[8] Appellants' Specification, in describing "a third aspect" of the invention, similarly describes the "computing entity" as "comprising: a computing
(Continued on next page.)

to the monitored computing entity?" (Br. 10.) The answer is that the claim does not recite performing a monitoring operation on the "computer entity." Instead, it recites "performing a monitoring operation of said *computer platform*" (emphasis added), which term the Examiner reads on Audebert's server Sap.

Appellants also argue that "the only thing monitored by the terminal . . . is the *data received from* the computing platform, not the *computing platform itself*" (*id.*). This argument is unpersuasive because the claim language "performing a monitoring operation of said computer platform" is broad enough to read on using terminal module 1 to monitor an operation of the computer platform (server Sap) by analyzing data received therefrom.

For the above reasons, we will sustain the rejection of claim 25 and dependent claims 26 and 28-31, which are not separately argued. *Nielson*, 816 F.2d at 1572.

Regarding independent claim 32,

> Applicants make note of the previous discussion respecting claim 25, and in particular that there is no monitoring operation conducted by the terminal of Audebert, and thus there is no possibility of reporting a result message to said token device, said result message describing a result of a monitoring operation, in the system of Audebert.

(Br. 11.) We assume this assertion that "there is no monitoring operation conducted by the terminal of Audebert" refers to the above-discussed claim 25 argument that "the only thing monitored by the terminal . . . is the *data*

---

platform . . . ; a monitoring component . . . ." (page 5, lines 16-18).

received from the computing platform, not the *computing platform itself*" (Br. 10). Not only is this argument unpersuasive for the reasons given above as applied to claim 25, which recites that "said monitoring component performing a monitoring operation of said computer platform," this argument is not commensurate in scope with claim 32, which does not identify the computer platform as the subject of the monitoring operation. Instead, claim 32 recites that "said monitoring component report[s] a result message to said token device, said result message describing a result of a monitoring operation." Consequently, we will sustain the rejection of claim 32 and the rejection of its dependent claims 33-37, which are not separately argued. *Nielson*, 816 F.2d at 1572.

Regarding independent claims 38, 42, and 43, Appellants (Br. 11-12) rely on the arguments already addressed above. We will therefore sustain the rejection of these claims.

DECISION

The rejection of claims 1, 2, 10-26, 28-32, 38, 42, 43, 45, 46, and 48-61 under 35 U.S.C. § 102(e) for anticipation by Audebert is sustained, as is the rejection of claims 3-9 and 33-37 under 35 U.S.C. § 103(a) for obviousness over Audebert in view of Perlman.

The Examiner's decision that claims 1-26, 28-38, 42, 43, 45, 46, and 48-61 are unpatentable over the prior art is therefore affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1). *See* 37 C.F.R. § 1.136(a)(1)(v) (2010).

AFFIRMED

babc

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528